REMARKS

In accordance with the foregoing, claims 1-4, 6-13, 17, 19-24, and 26-41 are amended. No new matter is added. Claims 5 and 25 are cancelled without prejudice. Claims 1-4, 6-24, and 26-41 are pending and under consideration.

CLAIM REJECTIONS UNDER 35 U.S.C. §103

In the outstanding Office Action, claims 1-41 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 5,113,383 to Amemiya et al. (hereinafter "Amemiya") in view of U.S. Patent No. 7,243242 to Moriai ("Moriai").

Independent claims 1, 20, 21, 40 and 41 are amended herewith to clarify the claimed subject matter. The amended claims specify that the claims recite "a hardware secure module having a tamper resistant module structure" which recitation is supported, for example, on page 10, lines 19-21 of the originally filed specification. In the amended claims, the term "second information" is replaced by "secure software" this amendment being supported, for example, by item 180 of FIGS. 2-5 and corresponding descriptions in the specification. The claims recite that the secure software is executed if the checking (comparison) should that the secure software is not falsified see, e.g. page 24, line 3 to page 25, line 17 or page 38, line 25 to page 39, line 2. The claims also further explicitly state that the reading of the secure software which is done by direct access is done "without using an operating system." (See, for example, page 13, line 13 to page 14, line 13.) Dependent claims are amended to use consistent language. No new matter is added.

Amemiya (a newly cited reference) discloses an information reproducing system for playing back a group of recording mediums according to programmed information, each recording medium having recorded information to be reproduced and Table of Contents (TOC) information with respect to the recorded information (see Amemiya's Abstract, Claim 1).

Moriai discloses a data terminal device capable of continuing to download encrypted content data and a license, or to reproduce encrypted content data while the data terminal's casing in the form of a shell is closed (see Moriai's Abstract).

Claim 1 is directed to an information reproducing apparatus having a hardware secure module, a memory, a falsification checking unit and a processor.

Amemiya and Moriai fail to disclose at least the following features recited in claim 1:

1. a hardware secure module having a tamper resistant module structure and storing information related to secure software;
2. a falsification checking unit that is loaded on the hardware secure module, wherein the falsification checking unit reads the secure software from the memory by direct access without using an operation system, compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison; and
3. a processor that executes the secure software when a result of the check by the falsification checking unit is that the secure software is not falsified.

Relative to (1) above, the Office Action submits that the primary reference, Amemiya does not disclose a secure module but relies on Moriai to disclose such a module. However, this bare identification of a secure module in Moriai depletes the alleged obvious prior art apparatus exactly of the security characteristic which the set-up aims to achieve. So Amemiya does not include a secure module and does not check whether the data has been falsified, i.e. no security of the data aspect is addressed in Amemiya. The absence of the secure module in Amemiya is not merely a minor departure from the structure of the apparatus in claim 1. The Office Action alleges that a person of ordinary skill in the art would integrate the secure module of Moriai in Amemiya's apparatus "to avoid third party viewing of the data as taught by Moriai." However, there is no evidence that Amemiya's apparatus would need such protection. Avoiding a third party access to the information is not a valid reason in the context put forth in Amemiya. None of the types of information compared in Amemiya, the Table of Content and the programmed information appears to have a special need to be securely protected.

Relative to (2) above, no secure features are implemented in Amemiya which builds a method solely for convenient managing of a stack of recordings (e.g. the CDs illustrated in FIG. 1a of Amemiya). Amemiya does not seek to check the integrity of the recordings on the CDs but merely whether it has all the information that would allow prompt access. In col. 12, lines 33-49 of Amemiya it appears that programmed information is used to control play-back of the recordings; if no appropriate programmed information for the recordings exists, the Table of Contents serves as basis to generate the programmed information.

As argued above, Amemiya is not concerned with security. Contrary to the assertion in the Office Action, in the indicated portion of Amemiya and in whole Amemiya's disclosure no "falsification checking unit that is loaded on the hardware secure module, wherein the falsification checking unit reads the secure software from the memory by direct access without using an operation system, compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison" is disclosed.

Additionally, the falsification checking unit as recited in claim 1 has the advantage that security against tampering or peeping appropriating functions of the operating system is higher because checking for any falsification/tampering is carried out directly accessing the memory without using the operating system.

Relative to (3), Amemiya and Moriai do not disclose a processor and as argued above neither other action taken based on the result of a security check. In Amemiya, if the programmed information used to control playing back the recordings exists, play-back starts immediately, but if the programmed information used to control playing back the recordings does not exists, then the programmed information is generated. FIGS. 9(a) to 9(d) in Amemiya are a flowchart of a play-back control sequence of an information reproducing system. Step S52 in FIG. 9(d) of Amemiya merely discloses "TRANSFER PROGRAMMED INFORMATION FROM CUMM TO PLAY." Applicants respectfully submit that Amemiya does not teach the processor recited in amended claim 1.

In view of the above arguments, claim 1 and claims 2-19 depending directly or indirectly from claim 1 patentably distinguish over the cited prior art. Claims 2-19 are patentable by inheriting patentable feature from claim 1 and by reciting additional patentable features. For example, Applicants found no evidence that the cited prior art references render obvious either that all information (i.e. secure software) is read to check falsification as recited in claim 2 or only a part of the information is read as recited in claim 3. Further, Applicants found no evidence that the cited prior art references render obvious that "the falsification checking unit performs the comparison [...] using a checksum method" as recited in claim 4. Applicants found no evidence that the cited prior art references render obvious that "the falsification checking unit the secure software from the memory on an irregular basis" as recited in claim 5. Applicants respectfully request the Examiner to analyze patentability of each claim on the merits.

In view of the above discussion relative to the prior art teachings, independent claim 20 patentably distinguishes over the cited prior art by reciting:

- reading secure software stored in a memory using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure which stores information related to the secure software;
- checking falsification by comparing the secure software with the information, and

determining whether the secure software is falsified based on a result of the comparison; and

- executing the secure software when result of determining is that the secure software is not falsified.

Independent claim 21 and claims 22-39 depending directly or indirectly from claim 21 patentably distinguishes over the cited prior art references at least because the following features recited in claim 21 are not rendered obvious as discussed above:

- a reading unit that reads a secure software from a memory mounted to the information reproducing apparatus by direct access without using an operating system; and
- a falsification checking unit that compares the secure software with information related to the secure software stored in the secure module, and checks a falsification of the secure software based on a result of the comparison, wherein if the result of the comparison shows that the secure software is not falsified the secure software is executed by the information reproducing apparatus.

Independent claim 40 patentably distinguishes over the cited prior art by reciting:

- reading secure software using a direct access method and without using an operating system, by the hardware secure module having a tamper resistant module structure storing information related to the secure software;
- checking falsification by comparing the secure software with the first information, and determining a falsification of the secure software based on a result of the comparison; and
- executing the secure software when the result of the comparison is that the secure software is not falsified.

Independent claim 41 patentably distinguishes over the cited prior art by reciting:

- executing secure software that is stored in a memory accessible to an information reproducing apparatus using a direct access method, if comparison of the secure software with information related to the secure software stored in a hardware secure module having a tamper resistant module structure inaccessible from outside, indicates that the secure software is not falsified.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Sept. 25, 2008

By: L Todor
Luminita A. Todor
Registration No. 57,639

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501